仮想通貨およびブロックチェーン技術 現状と課題

2018年11月29日（木） 14時～15時
（株）IT企画　才所敏明
toshiaki.saisho@advanced-it.co.jp
http://www.advanced-it.co.jp
https://www.facebook.com/toshiaki.saisho

 1

本日のお話

1. 仮想通貨とは（10分）
   法定通貨、電子マネー、ポイント/マイレージ、主要な仮想通貨
2. ブロックチェーンとは（10分）
   ブロックチェーンの特徴
3. ビットコインとそれを支える技術（20分）
   - 3.1 ビットコインとは
   - 3.2 ビットコインによる送金
   - 3.3 ビットコインのブロックチェーン
   - 3.4 ビットコイン・ウォレット
4. 仮想通貨・ブロックチェーンの現状・課題（15分）
   - 4.1 仮想通貨の課題
   - 4.2 仮想通貨の新潮流
   - 4.3 ブロックチェーンの新潮流

 2

自己紹介

1970年　東芝入社

社内計算機利用環境企画・構築・活用指導・支援
情報セキュリティ研究開発企画・推進、事業支援

2007年　（株）IT企画設立

事業支援活動（顧問・相談役）　2社（日、米）
大学教育活動（情報セキュリティ）　九大、慶応
研究開発活動（研究員）　中央大
暗号・認証、バイオメトリクス
電子メールセキュリティ、IoTシステムセキュリティ
FinTech（仮想通貨、ブロックチェーン他）
ビッグデータ、AI

1．仮想通貨とは

仮想通貨と法定通貨

（1）法定通貨（円やドル）は、国家単位で運営されている通貨
国が経済をコントロールするために発行・管理する貨幣。
国が価値を法律で保証することで、
国民は通貨と物やサービスを交換。
発行額の上限は決められていないが、
通貨の総量規制などにより国が経済をコントロールし
国民の安定した経済活動を支えている。

（2）仮想通貨（ビットコイン、イーサリアム）は、中央管理組織の無い通貨
紙幣や貨幣等の実体が存在しない通貨。
暗号技術が活用されており、暗号通貨とも呼ばれている。
ビットコインの場合、発行はすでに決められたネットワーク上の
プログラムに沿って自動的に行われ（現在：12.5BTC/10分）、
発行されるビットコインの数の上限（2100万BTC）がある。
各国の金融政策などで価値が左右されることがない。

1．仮想通貨とは

仮想通貨

改正資金決済法による「仮想通貨」の定義

一　物品を購入し、若しくは借り受け、又は役務の提供を受ける場合に、これらの**代価の弁済のために不特定の者に対して使用することができ**、かつ、**不特定の者を相手方として購入及び売却を行うことができる財産的価値**（電子機器その他の物に電子的方法により記録されているものに限り、本邦通貨及び外国通貨並びに通貨建資産を除く。次号において同じ。）であって、**電子情報処理組織を用いて移転することができるもの**　**（1号仮想通貨）**

二　不特定の者を相手方として前号に掲げるものと相互に交換を行うことができる財産的価値であって、電子情報処理組織を用いて移転することができるもの　**（2号仮想通貨）**

改正資金決済法による規制

顧客に対して仮想通貨を販売する販売所，交換所や，顧客の売り注文と買い注文をマッチングさせる場を提供する取引所を営む場合，**仮想通貨交換業の登録を受ける必要**がある。

 5

1．仮想通貨とは

電子マネーとポイント/マイレージ

（1）電子マネー

事業者により構築される**特定の経済圏内でのみ利用可能な通貨**。

「チャージ」という行為によって法定通貨を電子データに置き換え、持ち運びや決済が便利になった通貨。

電子マネーは、**法定通貨と同じ価値が電子化されたもの**。

参考：改正資金決済法（「資金決済に関する法律」）

事業者は残高の2分の1以上の保証金の供託義務。

（2）ポイント/マイレージ

事業者が、**顧客の囲い込みなどの目的のために発行するもの**で、サービスにかかるコストは、その事業者の利益により負担。

参考：景品表示法

取引価額の10分の2以内に規制。

 6

1．仮想通貨とは

仮想通貨概況

（1）2018年11月6日現在　約2100通貨が存在
時価総額　$214,948,381,954
全世界の法定通貨発行額の約2％に相当

（2）仮想通貨　時価総額ベスト10　（2018年11月6日現在）

順位	名称	記号	時価総額	
1	Bitcoin	BTC	$111,603,653,485	(52%)
2	Ethereum	ETH	$21,686,983,353	
3	XRP	XRP	$21,316,167,697	
4	Bitcoin Cash	BCH	$9,727,964,629	
5	EOS	EOS	$5,062,917,548	
6	Stellar	XLM	$4,788,815,193	
7	Litecoin	LTC	$3,206,426,163	
8	Cardano	ADA	$2,035,116,446	
9	Monero	XMR	$1,862,296,670	
10	Tether	USDT	$1,765,995,152	

 7

1．仮想通貨とは

主要な仮想通貨（1）

ビットコイン（BTC）　価格：512,982円/1BTC（11/22）価格推移
仮想通貨の中心的存在。分裂・派生した通貨も多い。
現在では最も単価が高く、最も人気のある通貨。
コンセンサスアルゴリズムは、PoW（Proof of Work）。
約10分間隔で1ブロック生成。マイニング報酬は12.5BTC。
（1日に約9億円分のBTCが発掘されている。）

イーサリアム（ETH）　価格：15,275円/1ETH（11/22）価格推移
ユーザが独自に定義できる契約（スマートコントラクト）の概念を導入。
柔軟なプラットフォームを提供。ICOプラットフォームとしても有名。
コンセンサスアルゴリズムは、PoW。　PoS（Proof of stake）へ移行予定。
約15秒間隔で1ブロック生成。マイニング報酬は3ETH。
（1日に約2.5億円のETHが発掘されている。）

 8

1．仮想通貨とは

主要な仮想通貨（2）

リップル（XRP）　価格：49.823円/1XRP（11/22）価格推移

送金/決済に特化した仮想通貨。リップル社が技術面で管理。
他の通貨と比べて送金速度に優れ、低コスト。
SBIとの共同事業が行われていて、日本人に人気が特に高い通貨。
コンセンサスアルゴリズムにRPCA採用。
（Ripple社が選んだ企業や団体が検証者）

ビットコイン・キャッシュ（BCH）　価格：34,035円/1BCH（11/22）価格推移

2017年8月1日にビットコインから分裂して誕生した仮想通貨。
ビットコインのブロック容量を1MBから32MBへ拡大し、
決済スピード（処理速度）を向上。
コンセンサスアルゴリズムは、PoW（Proof of Work）。

 9

ビットコインの価格推移
（2018年11月22日）

 10

ブロックチェーンは
記録を管理する技術

（1）中央管理組織の無い記録技術

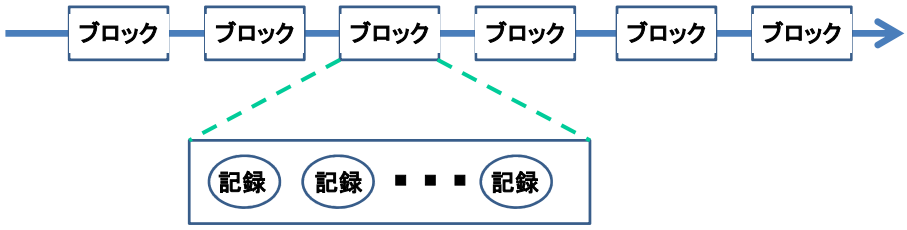
（2）過去の記録の改ざんが難しい記録技術

（3）記録消失の危険性が極めて低い記録技術

分散型台帳技術とも呼ばれている

ブロックチェーン

記録（支払等）を複数格納しているブロックの連鎖



2. ブロックチェーンとは

ブロックチェーンの特徴（1）
中央管理組織の無い記録技術

未登録の複数の記録を集めたブロックを構成し、
ブロックチェーンに追加（ブロックを承認）する人・組織の選定方法
をあらかじめ決めておくことが必要
＝＞ コンセンサスアルゴリズム

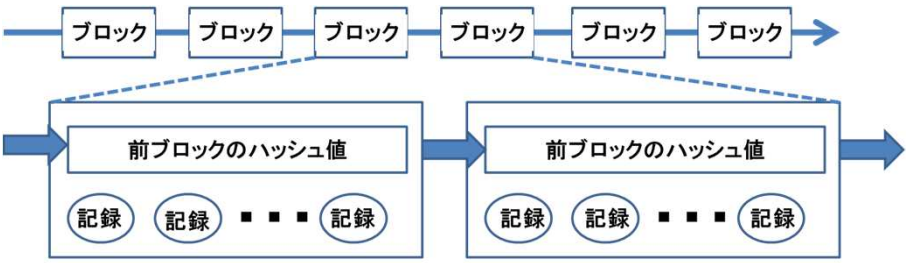
コンセンサスアルゴリズムの例（仮想通貨）
PoW（Proof of Work）：最初にマイニング（採掘）に成功した人に、承認権と報酬
マイニング：ブロックの構成要件を満たすナンス（数）を見出すこと
PoS（Proof of Stake）：保有量に応じて、承認権と報酬
PoI（Proof of Importance）：保有量に加えて、
記録生成（支払等）を活発にしている人・組織に、承認権と報酬

 13

2. ブロックチェーン技術とは

ブロックチェーンの特徴（2）
過去の記録の改ざんが難しい記録技術

過去の記録の情報（ハッシュ値）が
以降の記録に反映されているため



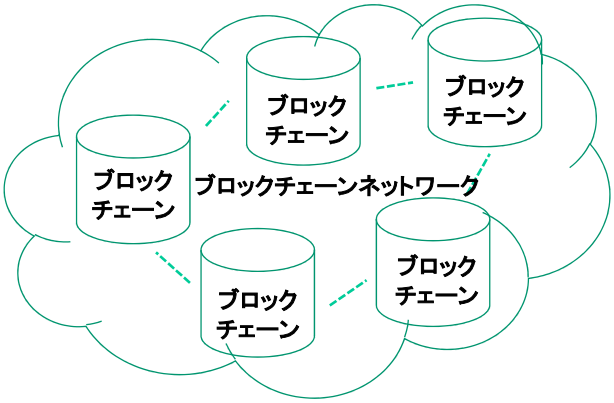
ハッシュ値：対象となるデータの特徴を一定の長さのデータに変換したもので、
対象となるデータが1ビットでも変われば、ハッシュ値も変わる。

 14

2. ブロックチェーン技術とは

ブロックチェーンの特徴（3）
記録消失の危険性が極めて低い記録技術

記録が多数のノードで保管・管理されているため



参考：ビットコインの場合、約1万ノードがブロックチェーンを保有

 15

3.1 ビットコインとは 40分

ビットコインの歴史

2008年10月　サトシ・ナカモト（Satoshi Nakamoto）が
インターネット上で論文投稿

2009年1月　ビットコインの理論を実現する
ソフトウェアがオープンソースで開発
（直後に、最初の取引が行われた）

2010年2月　ビットコイン両替ができる最初の取引所が誕生

2010年5月　現実世界ではじめてビットコインを使った決済
＜ピザ2枚（25ドル）と10000BTCの交換
➔ピザ2枚で約50億円分のBTCを入手！＞

 16

3.1 ビットコインとは

ビットコインの現状

ワレットユーザ（ビットコインアドレス）数　約2600万（7月現在）
　日本の取引所利用者登録数約200万、
　　アクティブユーザは半分程度か（2017年11月頃）

ブロックチェーンのサイズ　約140GB（2017年12月現在）
　フルノード数約1万（5月現在）、ブロック高約53.5万（8月5日）
　ブロックサイズ　1MB
　1ブロックあたり1000～2000トランザクション

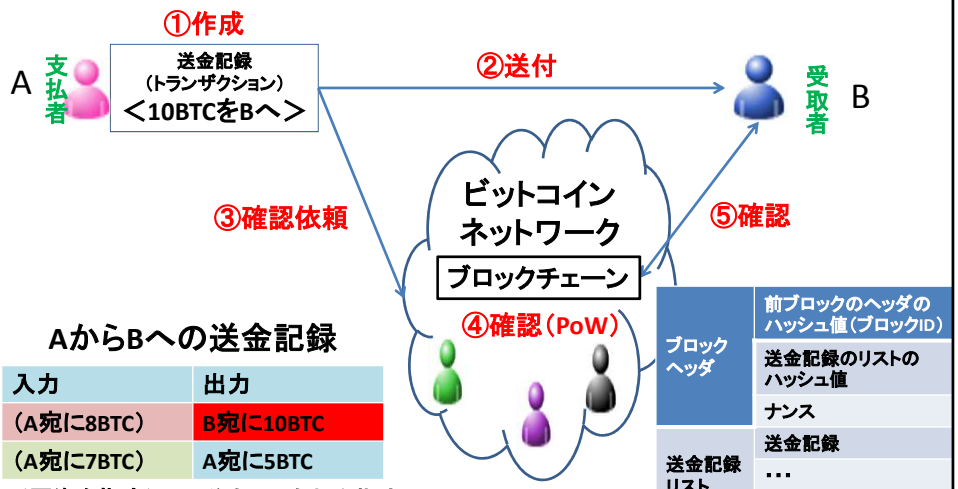
1BTCの相場　512,982円（11月22日現在　bitFlyer取引所）
　　約196,000円（2017年7月現在　bitFlyer取引所）

国内でビットコインが使える店舗　約52000店（3月現在）

 17

3.2 ビットコインによる送金

AからBへの10BTC送金の流れ



AからBへの送金記録

入力	出力
（A宛に8BTC）	B宛に10BTC
（A宛に7BTC）	A宛に5BTC
（原資を指定）	（送金先・金額を指定）

注：送金先は受取者のビットコインアドレスで指定

ブロックの構造

3.3 ビットコインのブロックチェーン

AからBへの10BTC送金のための Aによる新たな送金記録の作成

XからAへの送金記録（ID=n）

入力	出力
	A宛に8BTC

YからAへの送金記録（ID=m）

入力	出力
	A宛に7BTC

新規に作成する AからBへの送金記録

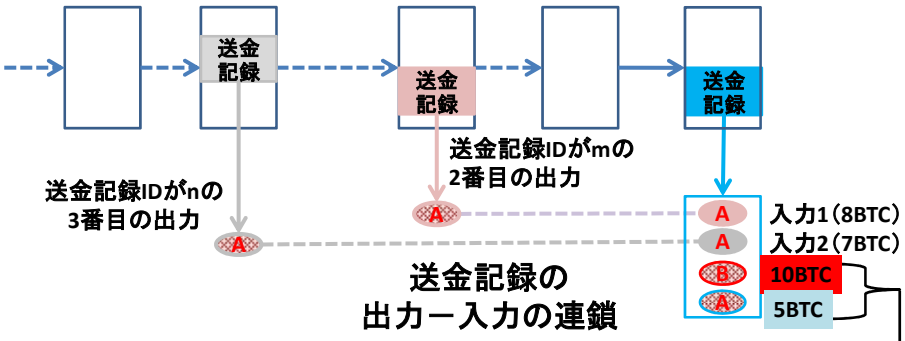
入力	出力
（A宛に8BTC）	B宛に10BTC
（A宛に7BTC）	A宛に5BTC

注1：原資は、送金記録IDおよび何番目の出力かにより指定
注2：送金記録IDは、送金記録のハッシュ値

ハッシュ値：対象となるデータの特徴を一定の長さのデータに変換したもの

3.3 ビットコインのブロックチェーン

ブロックチェーンにおける 送金記録の連鎖



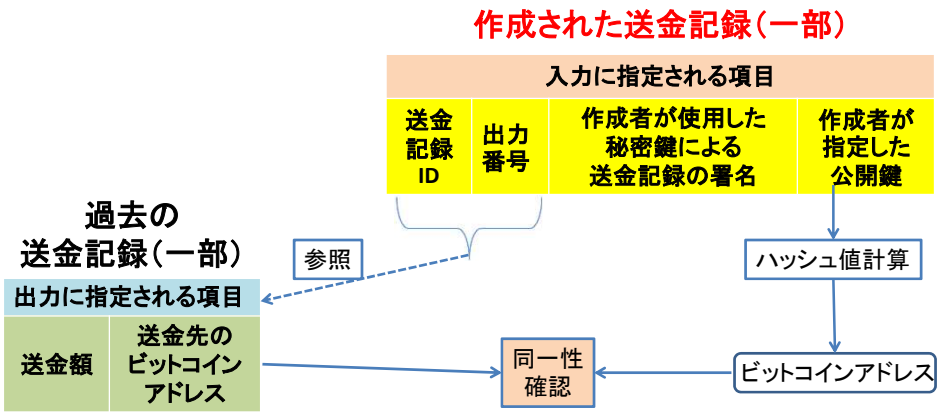
送金記録の出力ー入力の連鎖

入力の指定：
送金記録IDと何番目の出力かで指定
送金記録ID：
送金記録のハッシュ値

新規の出力
（使用可能なビットコイン）

3.3 ビットコインのブロックチェーン

作成された送金記録の検証（1）

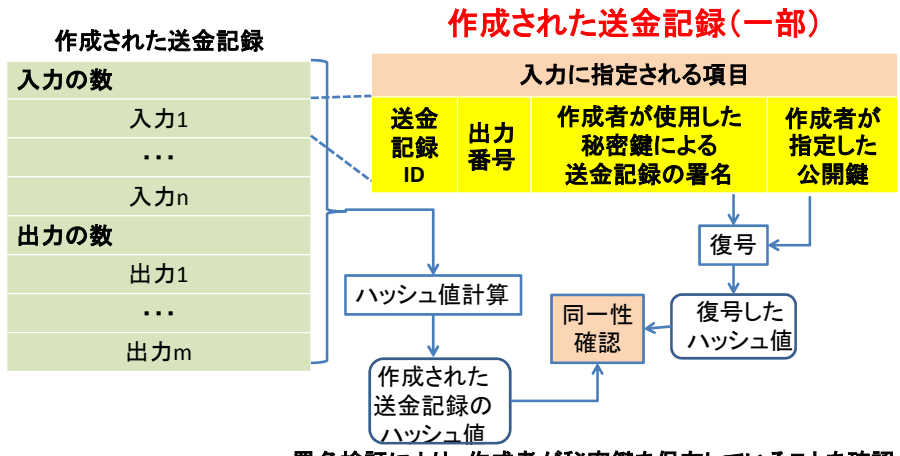


指定された出力の送金先のビットコインアドレスが
作成者が指定した公開鍵で生成されたビットコインアドレスかどうか、の確認

注：利用者のビットコインアドレスは、その人の公開鍵を一定のルールで変換したもの

3.3 ビットコインのブロックチェーン

作成された送金記録の検証（2）



署名検証により、作成者が秘密鍵を保有していることを確認

注1：ビットコイン利用者は、秘密鍵とそれに対応する秘密鍵を保有
注2：秘密鍵は利用者が秘密に管理すべき情報で、秘密鍵を持っていることが
　　対応する公開鍵/ビットコインアドレスの所有者であることの証明になる
注3：送信記録の署名は送信記録のハッシュ値を秘密鍵で暗号化したもの

3.3 ビットコインのブロックチェーン

作成された送金記録の検証のポイント

（1）指定された送金記録の出力が、作成者が指定した公開鍵に対応するビットコインアドレス宛ての出力（作成者宛の送金）かどうかの確認

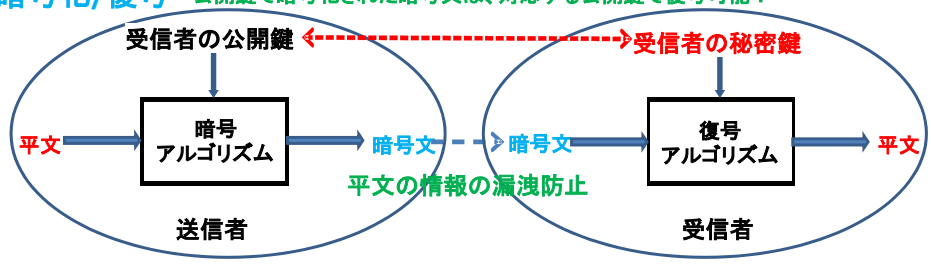
（2）指定された署名が、作成者の公開鍵に対応する正しい秘密鍵で作成された署名である（作成者が正しい秘密鍵を保有している）かどうかの確認

（3）本当に今も使用可能な送金記録の出力なのか？
（2重使用でないことの検査）
ブロックチェーン全体を確認し、
その出力が使用されていないことを確認

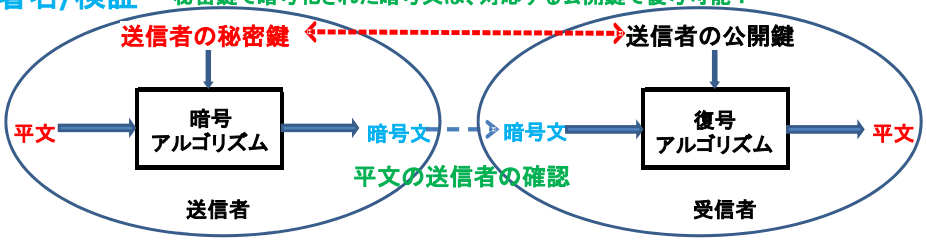
 23

補足説明：公開鍵暗号方式

暗号化/復号　公開鍵で暗号化された暗号文は、対応する公開鍵で復号可能！



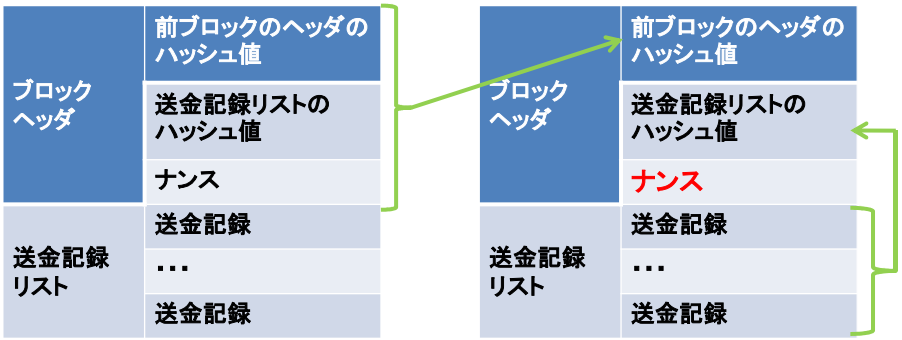
署名/検証　秘密鍵で暗号化された暗号文は、対応する公開鍵で復号可能！



 24

3.3 ビットコインのブロックチェーン

ビットコインブロックチェーンにおける ブロックの連鎖



マイナーは、それぞれ自分で構成したブロックに対し、マイニングを実施
ブロックのハッシュ値の先頭に16個0が並ぶようなナンスを発見する作業

3.4 ビットコイン・ウォレット

ビットコイン・ウォレットの機能

ビットコイン・ウォレットは、ビットコインの受取、支払、管理に使用

（1）受取：送金者に送金記録の出力欄の送金先として、
自分のビットコインアドレスを指定してもらう

（2）支払：送金記録の出力欄の送金先として、
相手のビットコインアドレスを指定する

（3）管理：ビットコインブロックチェーンを検索し、
送金先が自分のビットコインアドレスで
未使用の送金が含まれる送金記録を集め、管理する

（注）ビットコインアドレスは、所有者の公開鍵をベースに作成されている
正しい所有者かどうかの確認には、
対応する秘密鍵を保有しているかどうかで判断される
＜公開鍵と所有者の関連は公開されていないので、匿名性がある＞

3.4 ビットコイン・ウォレット

ビットコインウォレットの種類

（1）完全クライアント型
ブロックチェーンの全てのデータを
クライアントで管理（約140GB）（2017年12月現在）

（2）SPV（Simplified Payment Verification）クライアント型
各ブロックのヘッダしかクライアントでは管理しない（数十MB）

（3）サーバ・クライアント型
ブロックチェーンのデータはサーバ、秘密鍵はクライアントで管理

（4）Webサービス型
ソフトウェアのインストール不要、秘密鍵もWebサービス側で管理

 27

4.1 仮想通貨の課題 20分

多発する仮想通貨流出事件

（1）マウントゴックス事件（2014年2月） 内部犯行
概要：ビットコイン約75万BTC（当時のレートで約480億円）と
顧客が預けていた現金28億円が、仮想通貨取引所Mt.Goxから消失。
原因：当初サイバー攻撃によるものとされていたが、その後の警察の捜査の結果、
元社長であるマルク・カルプレスが業務上横領の疑いで逮捕された。

（2）Coincheck事件（2018年1月）
概要：仮想通貨取引所coincheckから約580億円相当の仮想通貨「NEM」が流出。
原因：システムの不備に対する不正アクセス
（ホットウォレットの使用、マルチシグの不使用）

（3）Zaif事件（2018年9月）
概要：仮想通貨取引所Zaifから約70億円相当の
仮想通貨「BTC、MONA、BCH」が流出」。
原因：システムの不備に対する不正アクセス （ホットウォレットのサーバが対象）

 28

4.1 仮想通貨の課題

仮想通貨規制の動き

背景　現在の仮想通貨の問題
　マネーロンダリング（資金洗浄）、テロリストへの資金流入
　ICO（Initial Coin Offering）まがいの詐欺の横行
　価格変動による金融システムの不安材料
仮想通貨への規制の動き
　中国：ICOの全面禁止、
　　国内3大取引所での仮想通貨と人民元の取引禁止（2017年9月）
　　国内でのマイニング事業の規制、マイニング工場は閉鎖（2018年1月）
　　習近平主席、ブロックチェーンの重要性に言及
　　（2018年5月の中国科学院・年次総会）、規制緩和の可能性？
　韓国：ICOの全面禁止（2017年9月）、金融監督院が国内仮想通貨取引所閉鎖検討
　　を発表（2018年1月）、その後、財務大臣が否定、規制緩和の可能性？
　日本：改正資金決済法の施行（2017年）
　　「仮想通貨交換業」としてのマネロン対策の義務化
　　「仮想通貨交換業等に関する研究会」（2018年3月）ICO規制等の検討
仮想通貨のルール作りには国際的な協力が必要（ドイツ、フランス）
　　3月のG20財務省・中央銀行総裁会議で規制案が提案された模様

 29

4.1 仮想通貨の課題

Bitcoin is harmful!

コンセンサスアルゴリズムは、PoW（Proof of Work）
　　世界中でマイニング競争➔膨大な無駄な計算
1件の送金処理に必要な電力消費量は、
　　VISAの4000倍以上が必要,　米国家庭9軒の1日分に相当
現在、ビットコインネットワークの
　　電力消費量は31 terawatt-hours/year
　　1日当たり450 gigawatt-hours増加中
　　（ハイチ（1085万）の全国の電力消費量の1年分に相当！）
現在のペースで電力使用量が増加すると・・・
　2019年7月までに、ビットコインネットワークは
　　米国全体の現在の電力を上回る電力を必要となる見込み
　2020年2月までに、ビットコインネットワークは
　　世界全体の現在の電力と同程度の電力を使用する見込み

 30

4.2 仮想通貨の新潮流

国家による仮想通貨発行
ベネズエラ・ボリバル共和国：Petro

背景：2017年当初今年初めに1ドル3000ボリバルであったのが、
2017年12月には103000ボリバルにまで通貨価値が下落

Petroは、自国の石油資源（世界一の埋蔵量）を担保に
イーサリアムのブロックチェーン上で発行された仮想通貨。

プリセール（ICO）は2018年1月に実施され、
時価総額50億ドル相当のトークンとなる予定

ベネズエラでの税金の支払い、公共サービス支払い、オンライン取引などに使用可能。ペトロの価格は理論上市場の原油価格と連動して推移するため、ベネズエラ国外に住む人は投機商品として利用することもできる。

多くの場所や用途で利用されることが予想され、少なくとも3100万人のベネズエラ国民が使用。世界における仮想通貨の利用人口よりはるかに多い。

 31

4.2 仮想通貨の新潮流

国家による仮想通貨発行
各国の動き

エストニア共和国：Estcoin
国家の仮想通貨となるのは無理か？
欧州中央銀行総裁は、ユーロ圏の通貨はユーロのみ、と発言
デジタル市民（e-Resident構想）向けのサービスで利用か？
ウルグアイ：eペソ（2017年11に試験運用開始）
ロシア：クリプトルーブル（プーチン大統領が発行指示？）
カナダ：CADコイン（Bank of Canadaが研究中）
オランダ：DNBコイン（De Nederlandsche Bankが研究中）
米国：Fedcoin（噂）

「世界中から紙幣が廃止されるのは、もはや時間の問題」
「全ての中央銀行は最終的には独自の暗号通貨を必要とするようになる」

 32

4.2 仮想通貨の新潮流

国家による仮想通貨発行 日本の動き

日本政府：「中央銀行によるデジタル通貨を発行する
可能性について検討して参りたい」（2018年2月安部首相）

金融機関： 1コイン＝約1円か
SBIホールディングス： Sコイン （2018年10月より実証実験？）
みずほ、ゆうちょ銀行： Jコイン （2020年頃？）
三菱東京UFJ銀行： MUFGコイン （2018年度？）

その他の企業：
楽天：楽天コイン （2019年ロシアで発行？）
サイバーエージェント （構想？）

地域仮想通貨：飛騨高山「さるぼぼコイン」、
大阪あべのハルカス「近鉄ハルカスコイン」
（地域通貨（地域振興券、プレミアム商品券）：1999年より、現在約600地域）

4.3 ブロックチェーン技術の新潮流

ビッグデータ対応：BlockchainDB

概要：
大企業が求める処理能力、大容量、および多様な検索・アクセス制御を提供するデータ管理機能に加え、
ブロックチェーンの特徴である記録データの不変性、分散コントロール、資産の登録・移転等の機能を提供

実現方式：ビッグデータ管理システム
（MongoDB：NoSQL DBMS）へブロックチェーンの特徴機能を付加

現状：世界で20社以上がパートナー企業となり、
応用PJが進行中（日本企業：リクルート、トヨタ）

4.3 ブロックチェーン技術の新潮流

IoT対応：IOTA

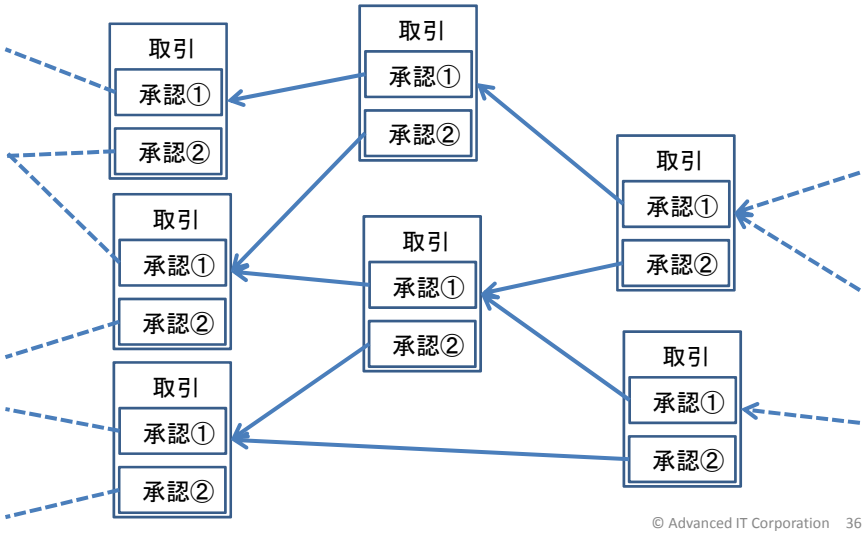
概要：機械と機械が直接取引を行うことを想定した、
IoT向けの仮想通貨/決済プロトコル
特徴は、マイナーが不要で、取引手数料がかからないこと

実現方式：ブロックチェーンでは無く、
Tangle（DAG：有向非巡回グラフ）を使用

現状：2017年11月、IOTA上で分散型データ販売市場確立のため
20社以上とパートナーシップ契約（マイクロソフト、富士通、
シスコ、フォルクスワーゲン、サムスン等）

4.3 ブロックチェーン技術の新潮流

Tangle（イメージ）



本日のお話

1. 仮想通貨とは（10分）
   法定通貨、電子マネー、ポイント/マイレージ、主要な仮想通貨
2. ブロックチェーンとは（10分）
   ブロックチェーンの特徴
3. ビットコインとそれを支える技術（20分）
   3.1 ビットコインとは
   3.2 ビットコインによる送金
   3.3 ビットコインのブロックチェーン
   3.4 ビットコイン・ウォレット
4. 仮想通貨・ブロックチェーンの現状・課題（15分）
   4.1 仮想通貨の課題
   4.2 仮想通貨の新潮流
   4.3 ブロックチェーンの新潮流

 37

終

2018年11月29日（木） 14時～15時
（株）IT企画　才所敏明
toshiaki.saisho@advanced-it.co.jp
http://www.advanced-it.co.jp/
https://www.facebook.com/toshiaki.saisho

 38